(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－23623
（P2002－23623A）
(43)公開日　平成14年１月23日(2002.1.23)

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ｂ　５Ｊ１０４

審査請求　未請求　請求項の数９　ＯＬ　（全 14 頁）

(21)出願番号　特願2000－212175(P2000－212175)

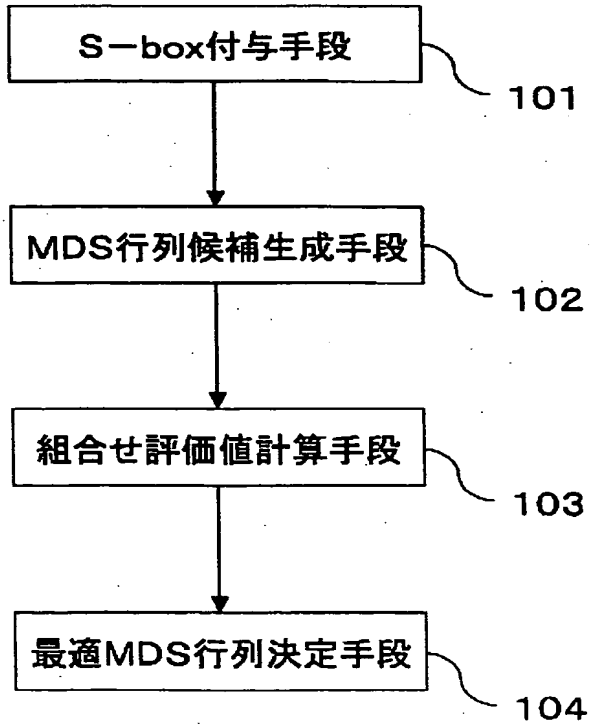
(22)出願日　平成12年７月13日(2000.7.13)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　村谷　博文
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　佐野　文彦
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(74)代理人　100083161
弁理士　外川　英明

最終頁に続く

(54)【発明の名称】　パラメータ決定装置、パラメータ決定方法、暗号化装置、および復号装置

(57)【要約】
【課題】　Ｓ－ｂｏｘとＭＤＳ行列を構成要素に含む暗号化装置において、Ｓ－ｂｏｘとＭＤＳ行列が、それぞれ、独立な設計方針により最適な複雑さを実現しようとしているにもかかわらず、相互に効果を相殺するで、かえってより安全ではない暗号化装置となってしまう恐れがあった。
【解決手段】　ＭＤＳ行列要素の各候補に対して、ある与えられたＳ－ｂｏｘに行列要素の乗算を行った結果の複雑さを評価し、この複雑さの評価結果に基づき、ＭＤＳ行列を構成する行列要素候補の組合せに対する複雑さの評価を与え、また、このＭＤＳ行列に対する逆行列に対しても同様の複雑さの評価を与え、これらの行列に対する複雑さの評価結果に基づき、そのＳ－ｂｏｘとの組合せにおいて、最適の複雑さを与えるＭＤＳ行列を決定する方法と、その方法によって得られたＭＤＳ行列を採用した暗号化装置を与える。



【特許請求の範囲】

【請求項１】　第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該拡散処理の前記第2パラメータを決定するためのパラメータ決定装置であって、
該換字処理に用いられる決定済みの第1パラメータを入力する入力手段と、
該拡散処理に用いられる第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、
該入力手段によって入力された第1パラメータと、該第2パラメータ候補生成手段によって逐次生成される各第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、
前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を前記装置の第2パラメータと決定する最適パラメータ決定手段とを備えたことを特徴とするパラメータ決定装置。

【請求項２】　第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該換字処理の前記第１パラメータを決定するためのパラメータ決定装置であって、
該換字処理に用いられる第1パラメータ候補を逐次生成する第1パラメータ候補生成手段と、
該拡散処理に用いられる決定済みの第2パラメータを入力する入力手段と、
該第1パラメータ候補生成手段によって逐次生成される各第1パラメータ候補と、該入力手段によって入力された第2パラメータとに基づいて、所定の方法によって評価値を逐次計算する計算手段と、
前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第1パラメータ候補を前記装置の第1パラメータと決定する最適パラメータ決定手段とを備えたことを特徴とするパラメータ決定装置。

【請求項３】　第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該換字処理の前記第１パラメータを決定するためのパラメータ決定装置であって、
該換字処理に用いられる第1パラメータ候補を逐次生成する第1パラメータ候補生成手段と、
該拡散処理に用いられる第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、
該第1パラメータ候補生成手段によって逐次生成される第1パラメータ候補と、
該第２パラメータ候補生成手段によって該拡散処理部行列候補生成手段によって逐次生成される第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、
前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第1パラメータ候補および第2パラメータ候補をそれぞれ前記装置の第1パラメータおよび第2パラメータと決定する最適パラメータ決定手段とを備えたことを特徴とするパラメータ決定装置。

【請求項４】　行列により平文の各文字間を置換する拡散処理を行う装置の、該拡散処理の前記行列を決定するために前記行列に最適な共通因子を決定するパラメータ決定装置であって、
該拡散処理に用いられる決定済みの行列を入力する入力手段と、
該拡散処理の行列に対し、括り出し可能な共通因子の候補を生成する共通因子候補生成手段と、
該共通因子候補生成手段によって逐次生成される共通因子候補によって該拡散処理の行列を括り出した後の行列に基づいて、所定の方法によって評価値を逐次計算する計算手段と、
該計算手段によって計算された評価値から最適な評価値を決定し、この決定した評価値に対応する共通因子候補を共通因子とする最適共通因子決定手段とを備えたことを特徴とするパラメータ決定装置。

【請求項５】　第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、パラメータ決定方法であって、該換字処理と該拡散処理との組み合わせによって定まる所定の方法にて計算された評価値が最適にするように第1パラメータあるいは第2パラメータあるいはそれら両方のパラメータを決定することを特徴とするパラメータ決定方法。

【請求項６】　第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、行列により平文の各文字間を置換する拡散処理とを行う装置の、該拡散処理の前記行列を決定するためのパラメータ決定装置であって、
該換字処理に用いられる決定済みの第1パラメータを入力する入力手段と、
該拡散処理に用いられる行列の一要素である第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、
該入力手段によって入力された第1パラメータと、該第2パラメータ候補生成手段によって逐次生成される各第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、
前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を前記行列の一要素の第2パラメータと決定する最適パラメータ決定手段とを備え、

前記行列の全ての要素を決定することを特徴とするパラメータ決定装置。

【請求項７】　前記最適パラメータ決定手段は、更に、得られた評価値から所定数の適した評価値を決定し、この決定した評価値に対応する第２パラメータ候補を前記行列の他の要素のパラメータ候補とすることを特徴とする請求項６のパラメータ決定装置。

【請求項８】　平文を暗号化するために、平文の各文字を別のものに変換する複数の換字処理部と、平文の各文字間を置換する拡散処理部とを備える暗号化装置であって、

前記拡散処理部は、

該換字処理部に用いられる決定済みの第1パラメータと、逐次生成される該拡散処理に用いられる第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算して得られた評価値の中から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を平文の各文字間の置換のために用いられるようにしたことを特徴とする暗号化装置。

【請求項９】　暗号文を復号するために、暗号文の各文字を別のものに変換する複数の換字処理部と、暗号文の各文字間を置換する拡散処理部とを備える復号装置であって、

前記拡散処理部は、該換字処理部に用いられる決定済みの第1パラメータと、逐次生成される該拡散処理に用いられる第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算して得られた評価値の中から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を平文の各文字間の置換のために用いられるようにしたことを特徴とする復号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、秘匿のためにデジタルデータを暗号化する暗号化装置、及び、必要に応じて復号するために用いる復号装置に関する。

【従来の技術】

【０００２】暗号系には、メッセージの暗号化と復号において同じ鍵を用いる秘密鍵暗号系と暗号化と復号で異なる鍵を用いる公開鍵暗号系がある。最も良く知られている秘密鍵暗号は、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）と呼ばれる米国標準ブロック暗号である。暗号解読は、平文（暗号化前のメッセージ）と暗号文（暗号化後のメッセージ）の対の集合から暗号化に用いられた鍵を求めることである。暗号解読には、平文がもともと持っていた冗長性（ｒｅｎｄｕｎｄａｎｃｙ）が利用されることが多い。

【０００３】Ｃｌａｕｄｅ　Ｅｌｍｗｏｏｄ　Ｓｈａｎｎｏｎは、“Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｔｈｅｏｒｙ　ｏｆ　Ｓｅｃｒｅｃｙ　Ｓｙｓｔｅｍｓ”（ＢｅｌｌＳｙｓｔｅｍ　Ｔｅｃｈｎｉｃａｌ　Ｊｏｕｒｎａｌ、２８巻４号、１９４９年、６５６－７１５）という論文の中で、平文（暗号化前のメッセージ）が持っている冗長性を見えにくくする技法を、ｃｏｎｆｕｓｉｏｎとｄｉｆｆｕｓｉｏｎの２つの基本的な技法に分類した。

【０００４】ｃｏｎｆｕｓｉｏｎとは、平文と暗号文の間の関係を見えにくくすることで、暗号文の冗長性や統計的パタンを観測することで解読を行うことを難しくする。例としては、平文のアルファベットの各文字を暗号文のアルファベットの各文字に対応付ける換字表を鍵として１字１字変換する方法、換字（ｓｕｂｓｔｉｔｕｔｉｏｎ）、がある。ｄｉｆｆｕｓｉｏｎとは、平文の冗長性を暗号文全体に広げることである。例としては、平文の文字の順序を置き換える転置（ｔｒａｎｓｐｏｓｉｔｉｏｎ）がある。

【０００５】先ほど述べたＤＥＳにおいても、暗号化処理は、Ｓ－ｂｏｘと呼ばれるｃｏｎｓｕｆｉｏｎの処理とＰ－ｂｏｘと呼ばれるｄｉｆｆｕｓｉｏｎ処理を基本的な処理として含んでいる。

【０００６】近年、ＤＥＳの後継暗号として、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）と呼ばれる次世代の米国標準ブロック暗号の仕様策定の作業が進められている。そこに提案された暗号は、ＤＥＳ以降の蓄積された暗号解読法の知見を反映して、ｃｏｎｆｕｓｉｏｎとｄｉｆｆｕｓｉｏｎにも新しい考え方が持ち込まれている。

【０００７】例えば、ｄｉｆｆｕｓｉｏｎの働きをする設計上の構成要素としては、線形変換の層が採用されることが多い。しかも、できるだけ効率良く拡散を行なうＭＤＳ（Ｍａｘｉｍａｌ　Ｄｉｓｔａｎｃｅ　Ｓｅｐａｒａｂｌｅ）符号を利用した線形変換層が提案されている。（Ｖｉｎｃｅｎｔ　Ｒｉｊｍｅｎ、Ｊｏａｎ　Ｄａｅｍｅｎ、“Ｔｈｅ　Ｃｉｐｈｅｒ　ＳＨＡＲＫ”、Ｆａｓｔ　Ｓｏｆｔｗａｒｅ　Ｅｎｃｒｙｐｔｉｏｎ、ＬＮＣＳ　１０３９、９９－１１２、１９９６。）

【０００８】このＭＤＳ符号を利用した線形変換層は、活性Ｓ－ｂｏｘ数の下限を保証する性質があるため、その事実を利用して、差分解読法と線形解読法に関する強度を証明することができるという特長がある。

【０００９】差分解読法と線形解読法以外の主な解読法に対する対策は、換字層において行われており、線形変換層に対する新たな制約とはならない。

【００１０】例えば、差分解読法、線形解読法、高階差分解読法、補間攻撃法に対して安全となるよう、Ｓ－ｂｏｘを有限体上のベキ関数やその和として設計する方法が提案されている。（盛合志帆、「差分／線形／高階差分／補間攻撃に対して強いＳ－ｂｏｘの一構成法」、１９９８年暗号と情報セキュリティシンポジウム、２．２．Ｃ、１９９８年。）

【００１１】また、補間攻撃に対して安全にするため、

有限体上のベキ関数と剰余類環上のアフィン変換によってＳ－ｂｏｘを構成する方法が提案されている。（M. Ｋａｎｄａ ｅｔ ａｌ.、“Ｅ２－Ａ Ｎｅｗ １２８－Ｂｉｔ Ｂｌｏｃｋ Ｃｉｐｈｅｒ”、ＩＥＩＣＥ Ｔｒａｎｓ. Ｆｕｎｄａｍｅｎｔａｌｓ.、Ｅ８３－Ａ、１、４８－５８、２０００。）

【００１２】つまり、現在の暗号設計の流儀では、差分解読法と線形解読法に対する対策としては、Ｓ－ｂｏｘの適切な選択とＭＤＳ符号を利用した線形変換層の採用が行われるものの、差分解読法や線形解読法以外の解読法に対する対策としては、主として、Ｓ－ｂｏｘの適切な選択によってのみ行われており、ＭＤＳ符号としてどのようなものを採用すべきか積極的な選択指針が与えられていない。

【００１３】ＭＤＳ符号を利用した線形変換層を行列として表現した場合、それをＭＤＳ行列と呼ぶことにする。ＭＤＳ行列の行列要素を決定する主な設計方針として、現在までに提案されているものの例は、ＡＥＳ候補であるＲｉｊｎｄａｅｌ暗号における設計方針としては、ＭＤＳ行列をテーブルルックアップで実装する場合のテーブルサイズを小さくすること、ＭＤＳ行列の行列演算を8ビットプロセッサで処理する場合に効率的に処理できること、がある。また、同じくＡＥＳ候補であるＴｗｏｆｉｓｈ暗号における設計方針としては、ＭＤＳ行列の直後で用いられているＰＨＴ（Ｐｓｅｕｄｏ－Ｈａｄａｍａｒｄ Ｔｒａｎｓｆｏｒｍａｔｉｏｎ）との関係から、ＭＤＳ行列が折角保証しているブランチ数をその直後のＰＨＴが小さくしてしまう確率を小さくするよう行列要素を決定している。

【００１４】つまり、従来、ＭＤＳ行列の行列要素の選択基準は、処理効率や実装コストの観点によるものが主である。例外は、ＰＨＴなど、他の特殊なプリミティブとの関連から差分解読法や線形解読法に対する安全性を極力下げないようにするというものであった。Ｒｉｊｎｄａｅｌ暗号の設計方針が言うように、8ビットプロセッサ上では、行列演算をテーブルルックアップではなく、プロセッサの算術演算や論理演算によって実装するため、タイミング攻撃に結びつく恐れもちろんあるため、行列要素を慎重に選択する必要があるという主張もあるのだが、特殊なプラットフォームに限定された問題と言える。

【００１５】従来のように、Ｓ－ｂｏｘとＭＤＳ行列を別々の設計方針で設計すると、Ｓ－ｂｏｘが折角安全性を高めるための設計をされているにもかかわらず、ＭＤＳ行列がその効果を相殺するような設計になってしまう恐れがある。

【００１６】例えば、Ｓ－ｂｏｘを出来るだけ複雑な関数として実現することで安全性を高めようとする場合を考える。例えば、ｎビットの入出力を持つＳ－ｂｏｘの場合、入出力をＧＦ（２ⁿ）の元とみなし、Ｓ－ｂｏｘをＧＦ（２ⁿ）からＧＦ（２ⁿ）への関数とするとき、その表現が単純な関数、具体的には、項数の少ない多項式や、分子の多項式の項数と分母の多項式の項数の和が小さい有理式、であるときには、補間攻撃が有効であることが知られている。（盛合志帆、下山武司、金子敏信、「ＳＮＡＫＥ暗号の補間攻撃」、１９９８年暗号と情報セキュリティシンポジウム、７．２．Ｃ、１９９８年。）補間攻撃とは暗号化関数を未知の係数を持つ多項式や有理式で表現し、平文ー暗号文の対を複数与えることで、これらの係数をラグランジュの補間法などによって決定する解読法である。

【００１７】補間攻撃を避けるために、Ｓ－ｂｏｘを構成する際に、単純なべき乗関数だけでなく、ＧＦ（２ⁿ）の代数構造に合わない処理、例えば、ビットの置換や別の代数構造における演算を利用する場合がある。この場合、Ｓ－ｂｏｘは、複数のべき乗関数による多項式として表現しなおすことができる。つまり、ＧＦ（２ⁿ）の代数構造とは異質な演算を組み合わせることで、実質的に、多項式の項数を増やした効果を得ている。

【００１８】この場合、Ｓ－ｂｏｘに続くＭＤＳ行列が、その入力の表現として、Ｓ－ｂｏｘの出力のＧＦ（２ⁿ）の表現と同じ表現を採用する場合には、ＭＤＳ行列の行列要素が乗算される影響は、Ｓ－ｂｏｘを表現しているべき乗関数の多項式の各項に対して、定数の乗算を行うに過ぎないので、Ｓ－ｂｏｘで項数を増やした効果を相殺するものとはならない。

【００１９】ところが、ＭＤＳ行列の入力の表現が、Ｓ－ｂｏｘの出力のＧＦ（２ⁿ）の表現とは異なる場合、例えば、ビット位置の役割が両表現で異なる場合や、ＭＤＳ行列の入力において意図的にビット置換が行われる場合などがそうであるが、この場合、折角Ｓ－ｂｏｘにおいて項数を増やすために行われた異質な演算の組合せの効果が、ＭＤＳ行列の演算において相殺されてしまう可能性がある。

【００２０】つまり、上の説明は、従来のように、Ｓ－ｂｏｘとＭＤＳ行列が、それぞれ、別個の設計方針で、独立に補間攻撃への対策を採ってしまうと、逆に、それらが相殺する恐れがあることを指摘するものである。

【００２１】次に、関数の複雑さを表す別の指標として、Ｓ－ｂｏｘの出力ビットを入力ビットの論理式で表した場合の項数も考えられる。この指標は、厳密な証明を与えることは難しいが、我々は、アバランシュ性の目安になると考える。

【００２２】アバランシュ性とは、入力が変化した場合に、その影響が出力の一部ではなく、できるだけ、広く影響する性質のことである。ビットの論理表現による項数が多ければ、出力ビットは、入力ビットに関して規則的な構造や、単純な表現となっていないと期待されるので、入力ビットの変化は、出力ビットに多様な変化をも

たらすことで高いアバランシュ性を実現できるのではないかと期待される。

【００２３】この場合においても、Ｓ－ｂｏｘとＭＤＳ行列が、それぞれ独立に、ビットの論理表現を複雑にするよう設計された場合に、その効果が相殺する場合がある。

【発明が解決しようとする課題】本発明は、Ｓ－ｂｏｘとＭＤＳ行列が別々の設計方針で設計されるために、折角Ｓ－ｂｏｘがある評価値で見たとき、安全性を高める設計をされているにも関わらず、ＭＤＳ行列がその効果を相殺するような設計になってしまうという課題があった。

【００２４】本発明は、このような問題点に鑑みてなされたものであり、暗号化装置または復号装置に適用する際に換字処理および拡散処理をできるパラメータ決定装置、パラメータ決定方法、暗号化装置、および復号装置を提供することを目的とする。

【課題を解決するための手段】上記目的を達成するために、本発明の請求項１のパラメータ決定装置は、第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該拡散処理の前記第2パラメータを決定するためのパラメータ決定装置であって、該換字処理に用いられる決定済みの第1パラメータを入力する入力手段と、該拡散処理に用いられる第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、該入力手段によって入力された第1パラメータと、該第2パラメータ候補生成手段によって逐次生成される各第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を前記装置の第2パラメータと決定する最適パラメータ決定手段とを備えた。

【００２５】また、本発明の請求項２のパラメータ決定装置は、第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該換字処理の前記第１パラメータを決定するためのパラメータ決定装置であって、該換字処理に用いられる第1パラメータ候補を逐次生成する第1パラメータ候補生成手段と、該拡散処理に用いられる決定済みの第2パラメータを入力する入力手段と、該第1パラメータ候補生成手段によって逐次生成される各第1パラメータ候補と、該入力手段によって入力された第2パラメータとに基づいて、所定の方法によって評価値を逐次計算する計算手段と、前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第1パラメータ候補を前記装置の第1パラメータと決定する最適パラメータ決定手段とを備えた。

【００２６】また、本発明の請求項３のパラメータ決定装置は、第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該換字処理の前記第１パラメータを決定するためのパラメータ決定装置であって、該換字処理に用いられる第1パラメータ候補を逐次生成する第1パラメータ候補生成手段と、該拡散処理に用いられる第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、該第1パラメータ候補生成手段によって逐次生成される第1パラメータ候補と、該第２パラメータ候補生成手段によって該拡散処理部行列候補生成手段によって逐次生成される第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第1パラメータ候補および第2パラメータ候補をそれぞれ前記装置の第1パラメータおよび第2パラメータと決定する最適パラメータ決定手段とを備えた。また、本発明の請求項４のパラメータ決定装置は、行列により平文の各文字間を置換する拡散処理を行う装置の、該拡散処理の前記行列を決定するために前記行列に最適な共通因子を決定するパラメータ決定装置であって、該拡散処理に用いられる決定済みの行列を入力する入力手段と、該拡散処理の行列に対し、括り出し可能な共通因子の候補を生成する共通因子候補生成手段と、該共通因子候補生成手段によって逐次生成される共通因子候補によって該拡散処理の行列を括り出した後の行列に基づいて、所定の方法によって評価値を逐次計算する計算手段と、該計算手段によって計算された評価値から最適な評価値を決定し、この決定した評価値に対応する共通因子候補を共通因子とする最適共通因子決定手段とを備えた。

【００２７】本発明の請求項５のパラメータ決定方法は、第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、パラメータ決定方法であって、該換字処理と該拡散処理との組み合わせによって定まる所定の方法にて計算された評価値が最適にするように第1パラメータあるいは第2パラメータあるいはそれら両方のパラメータを決定するようにした。

【００２８】また、請求項８の暗号化装置は、平文を暗号化するために、平文の各文字を別のものに変換する複数の換字処理部と、平文の各文字間を置換する拡散処理部とを備える暗号化装置であって、前記拡散処理部は、該換字処理部に用いられる決定済みの第1パラメータと、逐次生成される該拡散処理に用いられる第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算して得られた評価値の中から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補

を平文の各文字間の置換のために用いられるようにした。

【００２９】また、請求項９の復号装置は、暗号文を復号するために、暗号文の各文字を別のものに変換する複数の換字処理部と、暗号文の各文字間を置換する拡散処理部とを備える復号装置であって、

【００３０】前記拡散処理部は、該換字処理部に用いられる決定済みの第1パラメータと、逐次生成される該拡散処理に用いられる第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算して得られた評価値の中から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を平文の各文字間の置換のために用いられるようにした。

【００３１】これにより、暗号化装置または復号装置に適用する際に、性能の良い換字処理および拡散処理を有する暗号化装置および復号装置が提供できるようになった。

【発明の実施の形態】（第１実施形態）

【００３２】以下、図面を参照しながら発明の実施の形態を説明する。本実施形態では、与えられたＳ－ｂｏｘに対して、最適な組合せのＭＤＳ行列を決定する装置を示す。まず、本実施形態の基本的な構成例について説明する。

【００３３】図１に、本発明の一実施形態に係る、与えられたＳ－ｂｏｘに対して最適なＭＤＳ行列を決定する装置の構成を示す。

【００３４】図１に示されるように、本最適ＭＤＳ行列決定装置は、Ｓ－ｂｏｘ付与手段（１０１）とＭＤＳ行列候補生成手段（１０２）と組合せ評価値計算手段（１０３）と最適ＭＤＳ行列決定手段（１０４）とからなる。

【００３５】図２は、本実施形態による装置が行う処理の流れを表している。

【００３６】まず、Ｓ－ｂｏｘ付与手段は、本決定装置以外の装置によって決定された、あるＳ－ｂｏｘを指定する情報を受け入れる（２０１）。

【００３７】Ｓ－ｂｏｘは、一般には、ｍビット入力ｎビット出力の写像である。Ｓ－ｂｏｘの記述は、どのような入力値に対してどのような出力値を持つかを示す表として記述することも可能であるし、関数として簡潔な表現が可能であるならば、関数の形で記述することも可能である。ここでは、いずれにせよ、Ｓ－ｂｏｘを一意に特定できる情報が与えられるものとする。

【００３８】次に、ＭＤＳ行列候補生成手段は、当該付与されたＳ－ｂｏｘと組み合わせるＭＤＳ行列の候補を、逐次、生成する（２０２）。次に、組合せ評価値計算手段は、当該付与されたＳ－ｂｏｘと当該生成されたＭＤＳ行列候補の組合せの複雑度（評価値）を計算する（２０３）。次に、今計算したＭＤＳ行列候補が最後の候補であるか否かを判定する（２０４）。もし、まだ、新たな候補が存在する場合には、２０１の処理に戻り、新たなＭＤＳ行列の候補を生成する。こうして、逐次生成された、複数のＭＤＳ行列候補に対して同様の処理を繰り返し、その各々に対して組合せの複雑度を求める。

【００３９】ここで、組合せの複雑度とは、Ｓ－ｂｏｘとＭＤＳ行列候補の組合せに対する複雑度の意味で、Ｓ－ｂｏｘ単体、ＭＤＳ行列単体の複雑度ではなく、その両者の組合せを一体として評価した場合の複雑度である。具体的に、評価値である複雑度の例としては、Ｓ－ｂｏｘがｎビット入出力の場合、Ｓ－ｂｏｘの入出力をＧＦ（２^{n}）の元として表現するとき、Ｓ－ｂｏｘの入力で表現したＭＤＳ行列候補の出力の項数によって定義することができる。

【００４０】別の複雑度の例としては、ＧＦ（２^{n}）の元としてではなく、ビット毎に晴らしてみた場合、Ｓ－ｂｏｘの入力ビットによる論理式でＭＤＳ行列候補の出力ビットを表現した場合の項数をとる場合もある。２０４において、新たな候補が存在しない場合には、最後に、最適ＭＤＳ行列決定手段は、こうして求めた、当該付与Ｓ－ｂｏｘと当該生成された複数のＭＤＳ行列候補の各々の組合せの複雑度を元に、最適な組合せの複雑度を持つ組合せを決定し、そのＭＤＳ行列候補を最適なＭＤＳ行列として決定する（２０５）。この場合、評価値が複雑度である場合には、その値として項数が最大のものを選択する。

【００４１】ここでは、評価値として項数を例に挙げたが、それ以外の評価値を用いても同様の処理によって最適なＭＤＳ行列を決定する装置を実現することは容易である。

【００４２】図３は、より詳細に本実施形態の処理の流れを表す図である。まず、Ｓ－ｂｏｘの入力が行われる（３０１）。この入力されたＳ－ｂｏｘにおける出力を入力で表した多項式を求める（３０２）。次に、ＭＤＳ行列の行列要素候補として取りうる値を生成する（３０３）。ＭＤＳ行列の行列要素候補とは、ＭＤＳ行列がＧＦ（２^{n}）上の行列であれば、ＧＦ（２^{n}）の元を順々に生成すればよい。０は、ＧＦ（２^{n}）の元であるが、これを行列要素とすると行列はＭＤＳ行列にはなり得ないので、０を最初から除外して生成してもよい。

【００４３】次に、Ｓ－ｂｏｘの出力に、この行列要素候補を乗算した結果について、Ｓ－ｂｏｘの出力を入力で表した多項式を求める（３０４）。この多項式に基づき、Ｓ－ｂｏｘとこの行列要素候補の組合せに対する複雑度を計算する（３０５）。

【００４４】複雑度としては、Ｓ－ｂｏｘの入力やＳ－ｂｏｘの出力と行列要素候補の乗算結果をＧＦ（２^{n}）の元とみなして、Ｓ－ｂｏｘの入力の多項式として表現された乗算結果の項数を用いる。この項数による複雑度の定義については、後で、図４および図５によって詳細に説明する。もちろん、項数による複雑度の定義は、複

雑度の一例であって、様々な理論的根拠や経験的ヒューリスティックスによって別の複雑度の定義を用いても良い。例えば、多項式の次数にもとづいて複雑度を定義しても良い。また、別の、複雑度の例としては、有限体の元としてではなく、ビット単位で、出力ビットを入力ビットの多項式で表現した場合の項数によって複雑度を定義しても良い。その際、項数は、すべての次数の項数を同じ重みで数えてもよいし、多項式に含まれる項の次数に応じて重み付きで数えても良い。さらには、最適化がどのような攻撃法に対する安全性を達成することを目的としているかによっては、複雑度以外の評価値を定義しても良い。

【００４５】次に、まだ別の行列要素候補が存在するか否かを判定する（３０６）。まだ、別の候補が存在する場合には、３０３の処理にもどり新たな候補を生成して同様の処理を繰り返す。別の候補が存在しない場合には、行列要素候補の中から必要な個数の候補を選択し、ＭＤＳ行列候補を生成する（３０８）。

【００４６】この際、全ての行列要素候補の組合せによってＭＤＳ行列候補を生成すると、非常に多くの組合せの数があるため、すべてのＭＤＳ行列候補に対する複雑度の計算を行うことが非現実的となることがある。その場合には、３０５で計算した複雑度に従って、複雑度の大きないつくかの行列要素候補の集合の中から選ばれた行列要素候補によってＭＤＳ行列候補を生成することで、効率良く複雑度の大きなＭＤＳ行列を探索することも可能である（３０７）。この場合、ＭＤＳ行列候補の生成は、この絞り込まれた行列要素候補の中から行列要素を選択することによって生成される（３０８）。

【００４７】次に、こうして生成されたＭＤＳ行列候補が、実際に、ＭＤＳ行列となっているか否かを判定する（３０９）。この判定は、ＭＤＳ行列候補に対して、そのすべての小行列式が非零であることを確認することによって行われる。行列候補がＭＤＳ行列とならない場合には、３０８の処理にもどり、次の行列候補を生成して同様の処理を繰り返す。行列候補がＭＤＳ行列となっている場合は、行列の複雑度の計算を行う（３１０）。

【００４８】行列の複雑度は、３０６において求めたＳ－ｂｏｘと行列要素候補の組合せに対する複雑度を元に、ＭＤＳ行列候補に属する行列要素候補の各々に対する複雑度を足し合わせたものとして定義する。

【００４９】次に、逆行列を求める（３１１）。そして、逆行列に対しても３１０と同様にＳ－ｂｏｘと行列の組合せの複雑度を求める（３１２）。

【００５０】この場合、想定している暗号化処理や復号処理によっては、逆行列との組合せに用いるＳ－ｂｏｘは、もとのＳ－ｂｏｘの逆となるようにする変形例も可能である。

【００５１】こうして求めた、ＭＤＳ行列候補の複雑度とその逆行列の複雑度から、ともに、その複雑度が大きな候補を選択することで、最適なＳ－ｂｏｘとＭＤＳ行列の組合せを決定する（３１３）。

【００５２】上の例では、Ｓ－ｂｏｘと逆行列の組合せに関する複雑度まで評価したが、これを省略する変形例も可能である。その場合、３１１と３１２の処理は省略でき、３１３では、Ｓ－ｂｏｘとＭＤＳ行列の組合せの複雑度のみから最適な組合せを決定する。

【００５３】図４は、Ｓ－ｂｏｘと行列要素候補の組合せにおいて、出力を入力の多項式で表したときの複雑度を説明する図である。Ｓ－ｂｏｘの入出力が８ビットの場合の例である。４０１のＳ－ｂｏｘへの入力ビットをｉ０、ｉ１、…、ｉ７で表す。４０２の行列要素候補をＳ－ｂｏｘの出力に乗算した結果の出力ビットをｏ０、ｏ１、…、ｏ７と表す。入力と出力を有限体ＧＦ（２^8）上の元と見なし、ベクトル表現によって、それぞれ、$i=i_7z^7+i_6z^6+i_5z^5+i_4z^4+i_3z^3+i_2z^2+i_1z+i_0$、$o=o_7z^7+o_6z^6+o_5z^5+o_4z^4+o_3z^3+o_2z^2+o_1z+o_0$、と表現する。ここで、ｚは原始多項式$x^8+x^6+x^5+x+1=0$の根であるとする。評価値である複雑度は、例えば、ｏをｉの多項式として表現した場合における多項式の項数として定義される。別の定義としては、ｏをｉの有理式として表現した場合における分子の多項式の項数と分母の多項式の項数の和として定義することも可能である。これらの複雑度は、補間攻撃に対する耐性の目安となることが知られている。

【００５４】また、複雑度の別の定義としては、出力ビット、ｏ０、ｏ１、…、ｏ７、をビット毎に見て、それぞれ、入力ビットｉ０、ｉ１、…、ｉ７の論理式で表現した場合の項数をすべての出力ビットに関して和をとったものとして定義される。これは、この入出力間のアバランシュ性の目安となると思われる。また、間接的に、補間攻撃への耐性の目安にもあると思われる。

【００５５】図５は、Ｓ－ｂｏｘとＭＤＳ行列の組合せにおける複雑度の説明をする図である。

【００５６】５０１はＳ－ｂｏｘ、５０２はＭＤＳ行列で表現された拡散層を表している。例えば、ＧＦ（２^8）上のＭＤＳ行列の例で説明すると、その行列要素は、有限体ＧＦ（２^8）の元である。各Ｓ－ｂｏｘの出力は、この拡散層を通過することによって、ＭＤＳ行列の行列要素が乗算され、その結果を行方向に加算したものが拡散層の出力として現われる。この行列要素の乗算の部分だけを見ると、ちょうど、図４で説明した、Ｓ－ｂｏｘと行列要素候補の組合せとなっていることがわかる。そこで、Ｓ－ｂｏｘとＭＤＳ行列候補の組合せの複雑度を、図４を用いて説明したＳ－ｂｏｘと行列要素候補の組合せにおける複雑度を元に、ＭＤＳ行列候補の全ての行列要素に対して、この複雑度の求め、その結果を足し合わせたものとして定義する。この定義を用いると、Ｓ－ｂｏｘと行列要素候補の組合せの複雑度が求ま

っていれば、Ｓ－ｂｏｘとＭＤＳ行列候補の組合せに対する複雑度も求めることができる。

【００５７】Ｓ－ｂｏｘとＭＤＳ行列の組合せの複雑度に関するこの定義も、理論的根拠や経験的ヒューリスティックスによって異なる複雑度の定義を用いても良い。さらに、想定する攻撃法によっては、別の評価値の定義を用いて良い。

【００５８】ここで述べた複雑度の定義は例であって、これら以外にも、想定する攻撃法に応じて、理論的根拠と経験的ヒューリスティックスに基づいた多様な複雑度や評価値を定義して用いる場合にも、本発明を適用できる。例えば、コストや速度や他の攻撃に対する安全性の目安となる量を採用したとしても、換字層（Ｓ－ｂｏｘ）と拡散層（ＭＤＳ行列）の組合せでもって、その評価値を最適化することによって、拡散層のパラメータを最適となるよう決定するという変形例も可能である。

【００５９】図６は、以上に説明した装置によって、あるいは、別の方法や装置によって決定されたＭＤＳ行列による拡散層を極力小さな実装コストで実現したり、高速に動作するようにするために、ＭＤＳ行列の一部を括りだす装置の構成を示している。図７は、この装置の処理の流れを表している。

【００６０】ここで、括りだしとは、ＭＤＳ行列の同一行や同一列の属する行列要素から共通の因子を取り出す処理のことである。例えば、ＧＦ（２８）上の４行４列ＭＤＳ行列の第ｉ列の行列要素が、ａ１ｉ、ａ２ｉ、ａ３ｉ、ａ４ｉであるとすると、これから共通因子ａ（ここで、ａはＧＦ（２８）の非零元とする。）を括りだすとは、これらの行列要素に対して共通因子ａによる除算を行い、ｂ１ｉ、ｂ２ｉ、ｂ３ｉ、ｂ４ｉとすることである。ここで、ｂ１ｉ＝ａ１ｉ／ａ、ｂ２ｉ＝ａ２ｉ／ａ、ｂ３ｉ＝ａ３ｉ／ａ、ｂ４ｉ＝ａ４ｉ／ａである。このようにある列から共通因子を括り出すと行列が元の行列とは変ってしまうが、この共通因子ａをＭＤＳ行列の直前に置かれたＳ－ｂｏｘに対して繰り込むことで、Ｓ－ｂｏｘと行列全体としてみると、括りだし前と後は同じ処理となっている。

【００６１】ここで、因子ａをＳ－ｂｏｘに繰り込むとは、もともとのＳ－ｂｏｘが入力ｘを出力ｙ＝ｆ（ｘ）に変換する写像であるとすると、ａを繰り込んだＳ－ｂｏｘは入力ｘを出力ｙ’＝ａ×ｆ（ｘ）に変換する写像に変えることである。

【００６２】括りだしによって実装コストが小さくなる理由について説明する。ＭＤＳ行列のある列から括りだされた共通因子は、その列に入力しているＳ－ｂｏｘに対応している。そこで、ある列から括りだされた共通因子を、そのＳ－ｂｏｘに繰り込むことができる。Ｓ－ｂｏｘはテーブルルックアップによって実現されることが多い。この場合、この共通因子の繰り込みは、テーブルの値を変更するだけで済むので、テーブルの大きさを変えず、実装コストには影響しない。

【００６３】一方、ＭＤＳ行列は、一般に、テーブルサイズが大きくなるため、テーブルルックアップによって実現されるとは限らない。ハードウェアによる実装ならば結線によって、ソフトウェアならば命令の組合せによって実現することになる。この結線のコストや命令の組合せのコストは、共通因子括りだし後のＭＤＳ行列の行列要素の値に依存する。例えば、ＧＦ（２８）上の４行４列のＭＤＳ行列において、行列への入力をｘ１、ｘ２、ｘ３、ｘ４、行列の出力をｙ１、ｙ２、ｙ３、ｙ４、行列要素をａｉｊとする。ｙｉ＝ａｉ１×ｘ１＋ａｉ２×ｘ２＋ａｉ３×ｘ３＋ａｉ４×ｘ４である。例えば、ａｉ１が値として１を取るとき、ａｉ１×ｘ１の乗算は、ｘ１の各ビットの値がそのままａｉ１×ａ１の各ビットの値になるため、この乗算に相当するハードウェアはビット間の排他的論理和を行うための配線が不要である。同様にこの乗算に相当するソフトウェア命令の組合せもビット間の排他的論理和を行うためのビットシフト命令やマスク命令は不要である。つまり、ａｉ１が値１をとるときの実装コストは小さい。一般のａｉ１の値ではａｉ１×ａ１は、ビット間の排他的論理和を行う必要があり、その必要な回数はａｉ１の値によって異なる。したがって、実装コストは、行列要素の値によってことなる。このことから、共通因子の括りだしによって、実装コストの小さな行列要素からなるＭＤＳ行列への変換ができると、行列全体の実装コストは小さくて済む。

【００６４】結線やソフトウェア命令の組合せによって実現する場合のコストに対する評価値として、ファンインを定義する。ファインインは、行列要素の乗算において、乗算後の各ビットが乗算前の何個のビットの排他的論理和で表現されているかを数え、その結果をすべての行列要素について足し合わせたものとする。ファンインは、ＭＤＳ行列の行列要素の値によって決まるので、共通因子の括りだしによって、括りだし後の行列がファンインが小さな行列となっているならば、括りだした共通因子はＳ－ｂｏｘに繰り込み、残された行列を実際に結線やソフトウェア命令の組合せによって実現することで実装コストを小さくすることができる。

【００６５】図６が示すように、本装置は、ＭＤＳ行列付与手段（６０１）と共通因子候補生成手段（６０２）とコスト評価値計算手段（６０３）と最適共通因子決定手段（６０４）とからなる。

【００６６】図７は、このような最適な共通因子を見つけ出す装置の処理の流れを表している。まず、ＭＤＳ行列付与手段によって、ＭＤＳ行列が入力される（７０１）。次に、共通因子生成手段によって、括りだすべき共通因子の候補が生成される（７０２）。コスト評価値計算手段によって、この共通因子を括りだした後のＭＤＳ行列が計算される（７０３）。得られたＭＤＳ行列の

コスト評価値が計算される（７０４）。コスト評価値としては、例えば、先に述べたファンインがある。実装の方法によっては、別のコスト評価値を用いても良い。次に、括りだし後のＭＤＳ行列の逆行列を求める（７０５）。逆行列のコスト評価値を求める（７０６）。次に、まだ、別の共通因子の候補があるか判定する（７０７）。別の共通因子の候補がある場合には、７０２に戻り、新たな候補を生成し、以下同様の処理を行う。別の共通因子候補が無い場合には、最適共通因子決定手段が、それまでに求めたコスト評価値をもとに、最適な共通因子を決定する（７０８）。

【００６７】図７の例では、共通因子をＭＤＳ行列で括りだし、その括りだしの結果から逆行列のコスト評価値を計算したが、ＭＤＳ行列と逆行列でそれぞれ独立に共通因子のくくりだしを行うような変形も可能である。これは、暗号化の際のＳ－ｂｏｘと復号の際のＳ－ｂｏｘには、それぞれ、独立の共通因子を繰り込むことが可能であるからである。

【００６８】また、共通因子は、ＭＤＳ行列のすべての行列要素に共通の因子でも良いし、列毎あるいは行毎に異なる共通因子としても良い。

【００６９】これまでは、ＭＤＳ行列として最適なものを決定する装置の例を説明したが、図８は、ＭＤＳ行列が与えられた場合に、それと最適な組合せのＳ－ｂｏｘを決定する装置の構成を表している。図９は、その装置の処理の流れを表している。図１０は、より詳細にその装置の処理の流れを説明している。

【００７０】本装置は、ＭＤＳ行列付与手段（８０１）とＳ－ｂｏｘ候補生成手段（８０２）と組合せ評価値計算手段（８０３）と最適Ｓ－ｂｏｘ決定手段（８０４）とからなる。

【００７１】まず、ＭＤＳ行列付与手段は、本決定装置以外の装置によって決定された、あるＭＤＳ行列を指定する情報を受け入れる（９０１）。次に、Ｓ－ｂｏｘ候補生成手段は、当該付与されたＭＤＳ行列と組み合わせるＳ－ｂｏｘ候補を、逐次、生成する（９０２）。次に、組合せ評価値計算手段は、当該付与されたＭＤＳ行列と当該生成されたＳ－ｂｏｘ候補の組合せの複雑度（評価値）を計算する（９０３）。次に、今計算したＳ－ｂｏｘ候補が最後の候補であるか否かを判定する（９０４）。もし、まだ、新たな候補が存在する場合には、９０１の処理に戻り、新たなＳ－ｂｏｘ候補を生成する。こうして、逐次生成された、複数のＳ－ｂｏｘ候補に対して同様の処理を繰り返し、その各々に対して組合せの複雑度を求める。もし、９０４において、新たな候補が存在しない場合には、最適Ｓ－ｂｏｘ決定手段は、それまでに求めたＭＤＳ行列とＳ－ｂｏｘ候補の組合せの複雑度をもとに、最適な組合せを決定する（９０５）。

【００７２】より詳細に処理を説明する。まず、ＭＤＳ行列付与手段によって、ＭＤＳ行列の入力が行われる（１００１）。ＭＤＳ行列は各行列要素の値を与えることで一意に特定できる。

【００７３】次に、Ｓ－ｂｏｘ候補生成手段によって、Ｓ－ｂｏｘの候補の生成を行う（１００２）。

【００７４】ここで、Ｓ－ｂｏｘ候補の生成方法の例としては、Ｓ－ｂｏｘが入力値に対する出力値を表す表として記述できることより、相異なる値を持つ表を順次生成する方法がある。一般に、入出力のビット数が大きくなると、この方法で生成されるＳ－ｂｏｘの総数は非常に多くなるため、すべての可能性を生成することは非現実的となる。そこで、別の生成方法の例としては、生成されるＳ－ｂｏｘとして何らかの制約を課したものに限る方法がある。例えば、入力と出力をＧＦ（2^n）の元とみなしたとき、Ｓ－ｂｏｘを入力ｘのベキ乗関数x^kや異なるべきを持つべき乗関数の和$\Sigma c_k \times x^k$として表現できるものに限定して生成する方法も可能である。さらに、もう少し生成される個数を増やすならば、べき乗関数の和の前や後にビットの入れ替えを行ったものに制限して生成する方法も可能である。他には、アフィン変換などを組み合わせてもよい。

【００７５】次に、組合せ評価値計算手段は、生成されたＳ－ｂｏｘ候補における出力を入力で表した多項式を求める（１００３）。次に、Ｓ－ｂｏｘ候補とＭＤＳ行列の行列要素を乗算した結果について、Ｓ－ｂｏｘ候補の入力による多項式を計算する（１００４）。この多項式に基づき、Ｓ－ｂｏｘ候補と与えられたＭＤＳ行列の組合せに対する複雑度を計算する（１００５）。次に、ＭＤＳ行列の逆行列を求める（１００６）。

【００７６】１００６について、ＭＤＳ行列が与えられた１００１において、一度、逆行列を計算しておいて、あとで、その結果を繰り返し用いるような変形も可能である。

【００７７】次に、Ｓ－ｂｏｘ候補とこの逆行列に対して、多項式の計算を行う（１００７）。次に、Ｓ－ｂｏｘ候補と逆行列の組合せの複雑度を計算する（１００８）。次に、まだ別のＳ－ｂｏｘ候補が存在するか否かを判定する（１００９）。まだ、別の候補が存在する場合には、１００２の処理にもどり新たな候補を生成して同様の処理を繰り返す。別の候補が存在しない場合には、最適Ｓ－ｂｏｘ決定手段は、こうして求めた、Ｓ－ｂｏｘ候補とＭＤＳ行列の組合せの複雑度、Ｓ－ｂｏｘ候補とその逆行列の組合せの複雑度から、ともに、その複雑度が大きな候補を選択することで、最適なＳ－ｂｏｘとＭＤＳ行列の組合せを決定する（１０１０）。

【００７８】この場合において、１００６から１００８の処理を省略し、１０１０において、ＭＤＳ行列とＳ－ｂｏｘの組合せの複雑度のみから最適なＳ－ｂｏｘを決定する変形例が可能である。

【００７９】図３では、Ｓ－ｂｏｘは他の装置により決

定されたものを入力するとしたが、Ｓ－ｂｏｘについても、複数の候補のうち最適の組合せとなるものから選択する装置として実現する変形例も可能である。

【００８０】図１１は、図3の例に対して、Ｓ－ｂｏｘまで含めて最適な組合せを選択するように変形した装置の構成例を表す図である。図１２は、その処理の流れを表す図である。図１３は、さらに詳細にその処理を説明した図である。

【００８１】本変形例の装置は、Ｓ－ｂｏｘ候補生成手段（１１０１）とＭＤＳ候補生成手段（１１０２）と組合せ評価値計算手段（１１０３）と最適Ｓ－ｂｏｘおよびＭＤＳ行列決定手段（１１０４）とからなる。

【００８２】Ｓ－ｂｏｘ候補生成手段は、Ｓ－ｂｏｘの候補を生成する（１２０１）。次に、ＭＤＳ行列候補生成手段は、当該生成されたＳ－ｂｏｘ候補と組み合わせるＭＤＳ行列の候補を、逐次、生成する（１２０２）。次に、組合せ評価値計算手段は、当該生成されたＳ－ｂｏｘ候補と当該生成されたＭＤＳ行列候補の組合せの複雑度（評価値）を計算する（１２０３）。次に、今計算したＭＤＳ行列候補が最後の候補であるか否かを判定する（１２０４）。もし、まだ、新たな候補が存在する場合には、１２０２の処理に戻り、新たなＭＤＳ行列候補を生成する。こうして、逐次生成された、複数のＭＤＳ行列候補に対して同様の処理を繰り返し、その各々に対して組合せの複雑度を求める。もし、１２０４において新たなＭＤＳ行列候補が存在しないと判定した場合は、次にＳ－ｂｏｘ候補として新たな候補が存在するか判定する。もし、また、新たな候補が存在する場合には、１２０１に戻り、新たなＳ－ｂｏｘ候補に対して同様の処理を繰り返す。もし、１２０４において新たなＳ－ｂｏｘ候補が存在しないと判定した場合には、最適Ｓ－ｂｏｘおよびＭＤＳ行列決定手段は、これまでに求めたＭＤＳ候補とＳ－ｂｏｘ候補に対する複雑度をもとに最適なＭＤＳ行列とＳ－ｂｏｘの組み合せを決定する（１２０６）。

【００８３】より詳細に処理を説明する。まず、Ｓ－ｂｏｘ候補生成手段によって、Ｓ－ｂｏｘの候補の生成が行われる（１３０１）。組合せ評価値計算手段は、この生成されたＳ－ｂｏｘ候補における出力を入力で表した多項式を求める（１３０２）。次に、ＭＤＳ行列候補生成手段は、ＭＤＳ行列の行列要素の候補として取りうる値を生成する（１３０３）。組合せ評価値計算手段は、Ｓ－ｂｏｘ候補の出力に、この行列要素の候補を乗算した結果について、Ｓ－ｂｏｘ候補の入力による多項式を計算する（１３０４）。この多項式に基づき、Ｓ－ｂｏｘ候補とこの行列要素の候補の組合せに対する複雑度を計算する（１３０５）。複雑度としては、ＧＦ（２ｎ）の元とみなして、入力で表現した出力の多項式の項数を用いる。もちろん、項数を求める代わりに、多項式の次数によって複雑度を定義しても良い。また、別の、複雑度の例としては、出力ビットを入力ビットの多項式で表現した場合の項数で定義しても良い。その際、項数は、すべての次数の項数を同じ重みで数えてもよいし、次数に応じて重み付きで数えても良い。次に、まだ別の行列要素の候補が存在するか否かを判定する（１３０６）。まだ、別の候補が存在する場合には、１３０３の処理にもどり新たな候補を生成して同様の処理を繰り返す。別の候補が存在しない場合には、行列要素の候補の中から必要な個数の候補を選択し、ＭＤＳ行列の候補を生成する（１３０７）。

【００８４】実際、この候補がＭＤＳ行列となっているか否かを判定する（１３０８）。この判定は、ＭＤＳ行列の候補が、すべての小行列式が非零であることを確認することによって行われる。行列候補がＭＤＳ行列とならない場合には、１３０７の処理にもどり、次の行列候補を生成して同様の処理を繰り返す。行列候補がＭＤＳ行列となっている場合は、行列の複雑度の計算を行う（１３０９）。これは、１３０５において求めたＳ－ｂｏｘ候補と行列要素の候補の組合せに対する複雑度を元に、行列候補に属する行列要素の候補に対する複雑度を足し合わせることで計算する。次に、逆行列を求める（１３１０）。

【００８５】そして、逆行列に対しても１３０９と同様に行列の複雑度を求める（１３１１）。次に、Ｓ－ｂｏｘ候補としてこれが最後であるか否かを判定する（１３１２）。もし、まだ新たなＳ－ｂｏｘ候補が存在する場合には、１３０１に戻り新たなＳ－ｂｏｘ候補を生成して、同様の処理を繰り返す。最後のＳ－ｂｏｘ候補の場合には、最適Ｓ－ｂｏｘ及びＭＤＳ行列決定手段は、Ｓ－ｂｏｘ候補とＭＤＳ行列候補の組合せのうち、Ｓ－ｂｏｘ候補とＭＤＳ行列の組合せの複雑度と、Ｓ－ｂｏｘと逆行列の組合せの複雑度のいずれもが大きな複雑度となるものを最適なＳ－ｂｏｘとＭＤＳ行列の組合せと決定する（１３１３）。

（第２実施形態）

【００８６】次に、図１４は、以上に述べたＳ－ｂｏｘとＭＤＳ行列の最適な組合せを与える装置によって決定されたＳ－ｂｏｘやＭＤＳ行列を採用する暗号化装置の構造を表す図である。１４０１は、暗号化装置のデータ撹拌を行う部分を表しており、平文を入力して暗号文を出力する。１４０１は、その構造の一部として、例えば、複数のＳ－ｂｏｘによって構成される換字層１４０３と、例えば、ＭＤＳ行列によって構成される拡散層１４０４を持つ。拡散層８０４は換字層８０３に直列に接続している。１４０２はデータ撹拌部のうち１４０３と１４０４以外の残りの暗号化処理部分である。１４０２の中にも１４０３と１４０４と同じ構造が含まれていても良い。

【００８７】ここで、換字層１４０３と拡散層１４０４は、その一方もしくはその両方が、第１実施形態におい

て説明されたＳ－ｂｏｘまたはＭＤＳ行列またはその両方を決定する装置によって決定されたパラメータを持つ。これにより、１４０１のデータ攪拌文は、補間攻撃に対する安全性に優れたものであったり、アバランシュ性の良いものであったり、第１実施形態において選択した評価値の定義が意図していた望ましい性質に関して最適なＳ－ｂｏｘとＭＤＳ行列の組合せを与えるものとなっている。

【００８８】このデータ攪拌部１４０１の動作について説明すると、平文が１４０１に入力されると、その入力は各種の変換を受けつつ、やがて、１４０２から換字層１４０３へと入力が渡される。換字層１４０３は、複数のＳ－ｂｏｘで構成されており、各Ｓ－ｂｏｘは受け取った入力に対して換え字を行った結果を出力する。Ｓ－ｂｏｘの出力は、次の拡散層へと入力される。拡散層１４０４はＭＤＳ行列として表現され、拡散層１４０３からの入力に対して行列演算を施した結果を出力し、その出力を残りの暗号化処理部１４０２に返す。残りの暗号化処理部は、拡散層１４０４から受け取ったデータに対してさらなる変換を行い、最終的には暗号文として出力する。

【００８９】ここでは、残りの暗号化部１４０２は、ひとつの部分からなる構造として表現されているが、換字層１４０３より前の部分と拡散層１４０４より後の部分の２つに分離した構造をしていても良い。また、その一方は、無くてもよい。

【００９０】さらに、説明では換字層１４０３と拡散層１４０４は直結していたが、両者の間に例えば、拡大鍵加算のような別の処理が挟まっていても良い。拡大鍵加算は、拡散層１４０４と順序を交換することで、線形変換によって得られる別の値の拡大鍵を１４０４の後に加算するのと同等であるからである。

【００９１】なお、以上の実施形態の説明においては、換字層の後に拡散層が続く例によって最適な組合せを決定する方式を例にとって説明を行ったが、拡散層の後に換字層が続く場合や、複数の換字層が続く場合、複数の拡散層が続く場合、換字層と拡散層が任意の順で任意の数ずつ交互に積み重なる場合、などにおいても、同様に、組合せの評価値を求めて最適化を行う変形例も可能である。

【００９２】本発明の各実施形態は、装置による実施形態を述べたが、汎用のコンピュータ上で動作するソフトウェアプログラムとしても実現可能である。

【発明の効果】

【００９３】以上説明したように本発明によれば、従来、Ｓ－ｂｏｘとＭＤＳ行列を構成要素に含む暗号化装置において、Ｓ－ｂｏｘとＭＤＳ行列が、それぞれ、独立な設計方針により最適な複雑さを実現しようとしているにもかかわらず、相互に効果を相殺するで、かえってより安全ではない暗号化装置となってしまう恐れがあったが、ＭＤＳ行列要素の各候補に対して、ある与えられたＳ－ｂｏｘに行列要素の乗算を行った結果の複雑さを評価し、この複雑さの評価結果に基づき、ＭＤＳ行列を構成する行列要素候補の組合せに対する複雑さの評価を与え、また、このＭＤＳ行列に対する逆行列に対しても同様の複雑さの評価を与え、これらの行列に対する複雑さの評価結果に基づき、ある与えられたＳ－ｂｏｘと組合せにおいて、最適の複雑さを与えるＭＤＳ行列を決定することによって、互いの効果が相殺しない最適な組合せを決定することができるようになり、ひいては、そのように決定されたＳ－ｂｏｘやＭＤＳ行列を採用したより安全な暗号化装置を与えることができる。

【図面の簡単な説明】

【図１】本発明における与えられたＳ－ｂｏｘに対して最適な組合せのＭＤＳ行列を決定する装置の構成を表す図。

【図２】本発明における与えられたＳ－ｂｏｘに対して最適な組合せのＭＤＳ行列を決定する装置の処理を表す図。

【図３】本発明における与えられたＳ－ｂｏｘに対して最適な組合せのＭＤＳ行列を決定する装置の処理の詳細を表す図。

【図４】Ｓ－ｂｏｘと行列要素候補の組合せにおける複雑度を表す図。

【図５】Ｓ－ｂｏｘとＭＤＳ行列の組合せにおける複雑度を表す図。

【図６】本発明における与えられたＭＤＳ行列に対して最適な共通因子を決定する装置の構成を表す図。

【図７】本発明における与えられたＭＤＳ行列に対して最適な共通因子を決定する装置の処理を表す図。

【図８】本発明における与えられたＭＤＳ行列に対して最適な組合せのＳ－ｂｏｘを決定する装置の構成を表す図。

【図９】本発明における与えられたＭＤＳ行列に対して最適な組合せのＳ－ｂｏｘを決定する装置の処理の詳細を表す図。

【図１０】本発明における与えられたＭＤＳ行列に対して最適な組合せのＳ－ｂｏｘを決定する装置の処理の詳細を表す図。

【図１１】本発明における最適なＳ－ｂｏｘとＭＤＳ行列の組合せを決定する装置の構成を表す図。

【図１２】本発明における最適なＳ－ｂｏｘとＭＤＳ行列の組合せを決定する装置の処理を表す図。

【図１３】本発明における最適なＳ－ｂｏｘとＭＤＳ行列の組合せを決定する装置の処理の詳細を表す図。

【図１４】本発明における最適なＳ－ｂｏｘまたはＭＤＳ行列またはその両方を用いた暗号化装置を表す図。

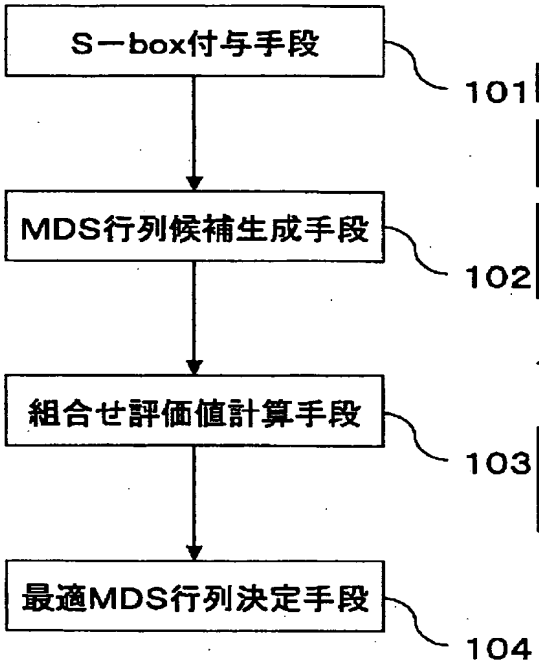
【符号の説明】

１０１　Ｓ－ｂｏｘ付与手段

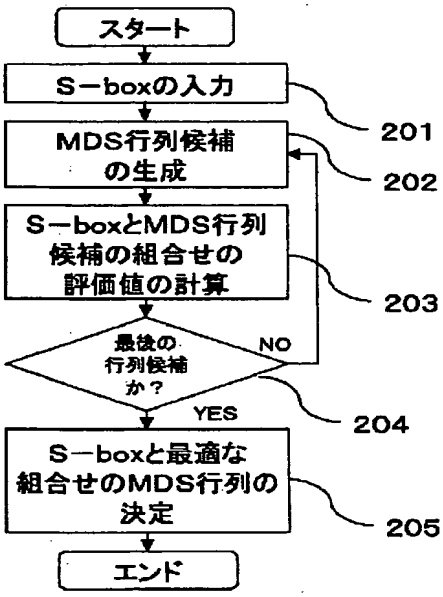
１０２　ＭＤＳ行列候補生成手段

１０３　組合せ評価値計算手段
１０４　最適ＭＤＳ行列決定手段
４０１　Ｓ－ｂｏｘ
４０２　行列要素候補
５０１　Ｓ－ｂｏｘ
５０２　ＭＤＳ行列
６０１　ＭＤＳ行列付与手段
６０２　共通因子候補生成手段
６０３　コスト評価値計算手段
６０４　最適共通因子決定手段
８０１　ＭＤＳ行列付与手段
８０２　Ｓ－ｂｏｘ候補生成手段
８０３　組合せ評価値計算手段
８０４　最適Ｓ－ｂｏｘおよびｍｄｓ行列決定手段
１１０１　Ｓ－ｂｏｘ候補生成手段
１１０２　ＭＤＳ行列生成手段
１１０３　組合せ評価値計算手段
１１０４　最適Ｓ－ｂｏｘおよびＭＤＳ行列決定手段
１４０１　暗号化処理部（データ撹拌部）
１４０２　その他の暗号化処理部
１４０３　Ｓ－ｂｏｘ
１４０４　ＭＤＳ行列

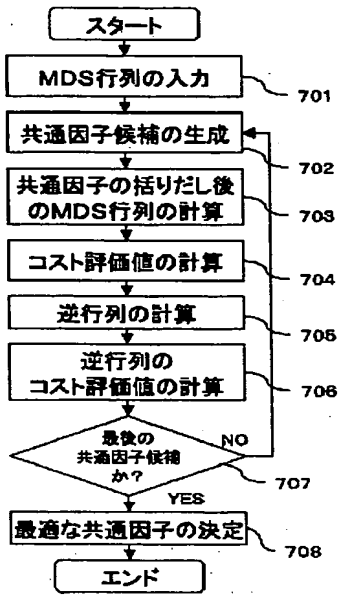
【図１】



【図２】

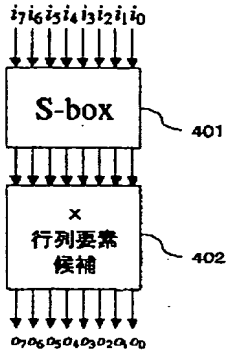


【図７】



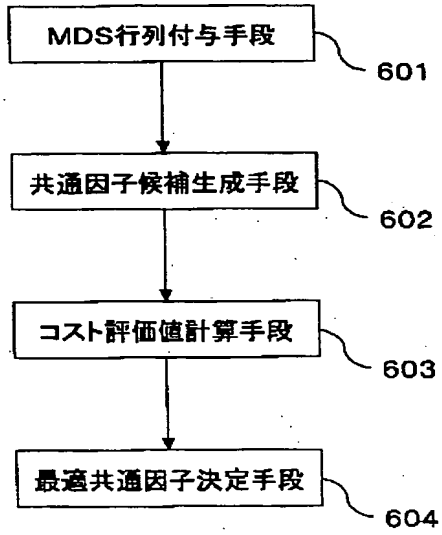
【図４】

$$i = i_7 z^7 + i_6 z^6 + i_5 z^5 + i_4 z^4 + i_3 z^3 + i_2 z^2 + i_1 z + i_0$$

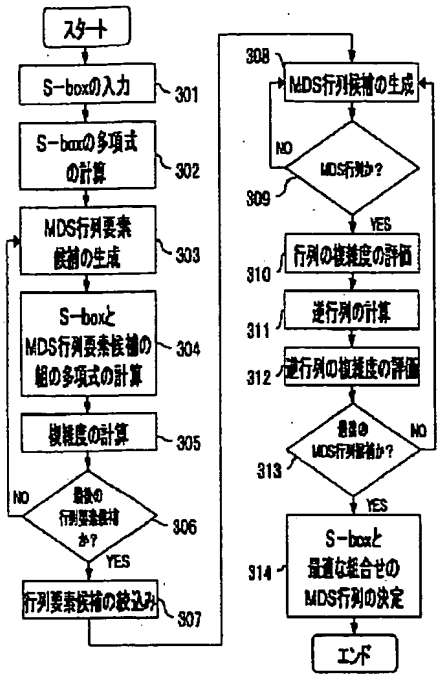


$$o = o_7 z^7 + o_6 z^6 + o_5 z^5 + o_4 z^4 + o_3 z^3 + o_2 z^2 + o_1 z + o_0$$

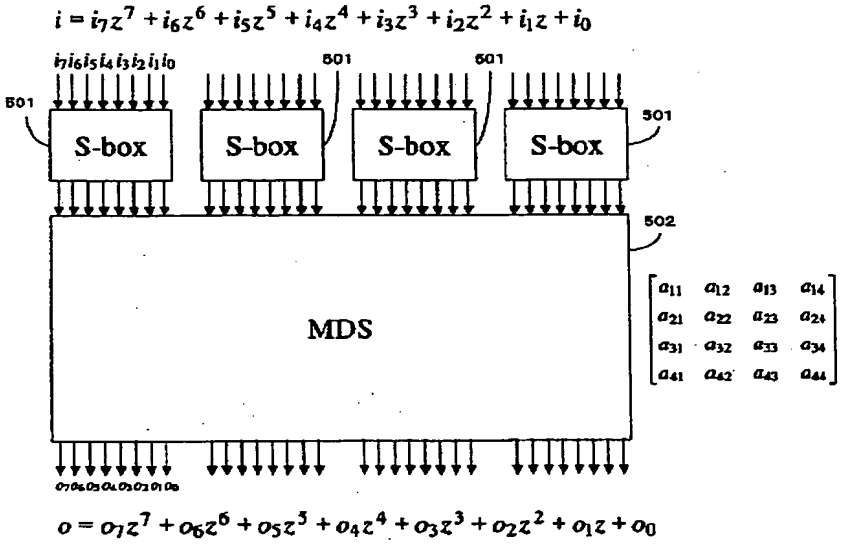
【図６】



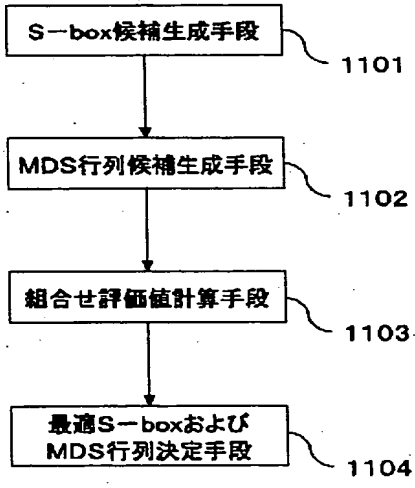
【図３】



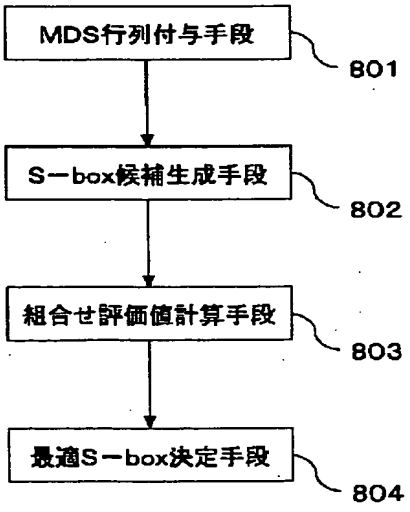
【図５】



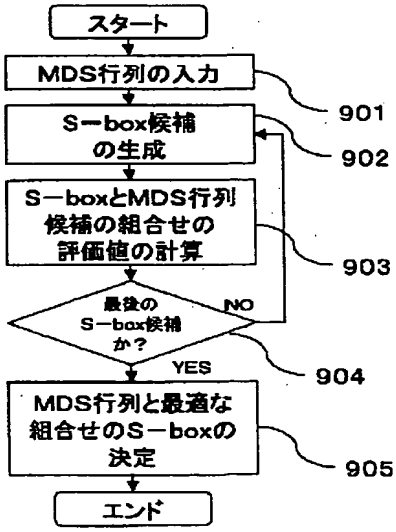
【図１１】



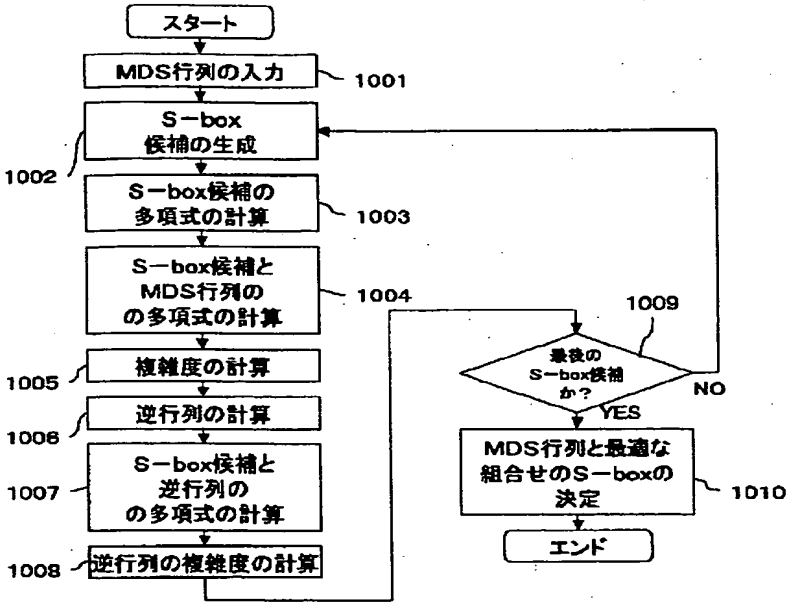
【図８】



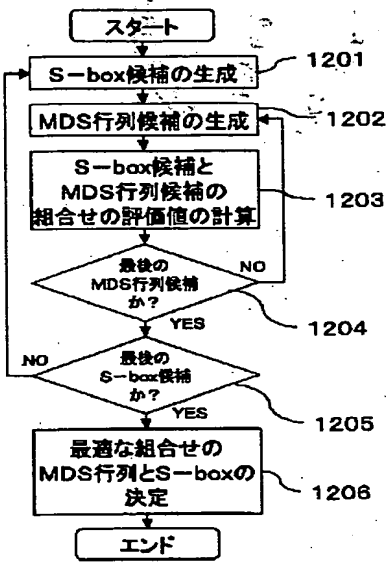
【図９】



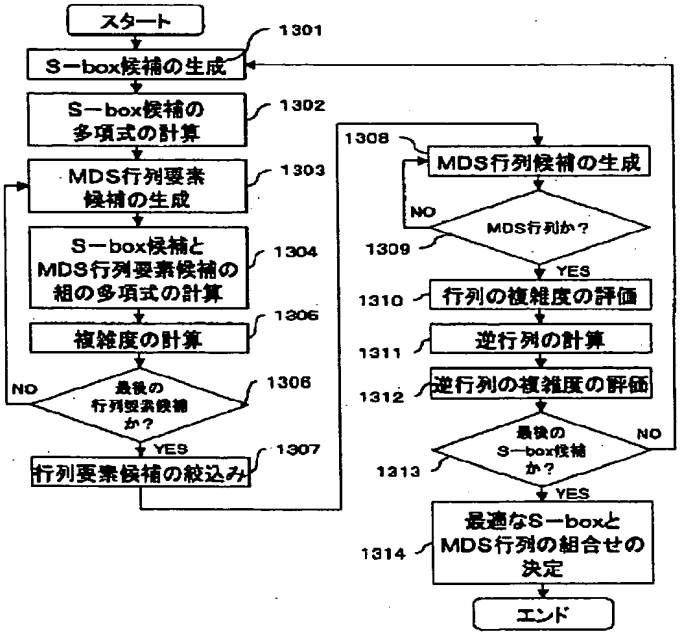
【図１０】



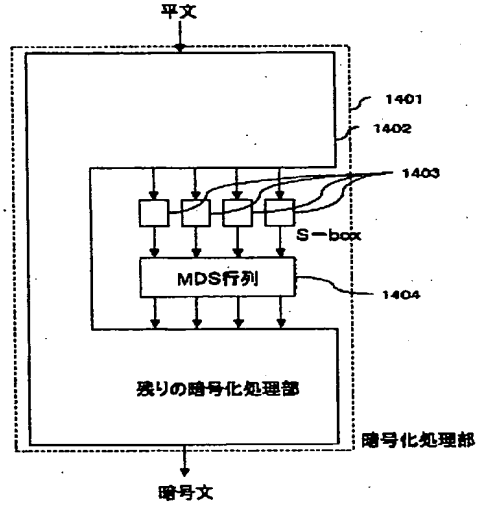
【図１２】



【図１３】



【図１４】



フロントページの続き

(72)発明者　大熊　建司
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　川村　信一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

Ｆターム(参考)　5J104 AA41 JA09 JA17 NA08 NA10